(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04L 12/28

(11) 공개번호 특2001-0087322
(43) 공개일자 2001년09월15일

(21) 출원번호 10-2001-0011042
(22) 출원일자 2001년03월03일
(30) 우선권주장 09/518,399 2000년03월03일 미국(US)
(71) 출원인 넥스랜드, 인코퍼레이티드 추후제출
미합중국, 33180 플로리다, 마이아미, 슈트 403, 비스케인 블러바드 20801
(72) 발명자 술탄,이스라엘다니엘
프랑스,파리75013,뤼까이오9
(74) 대리인 조문현, 김영철, 김 순 영, 이준서

심사청구 : 없음

(54) 로컬 아이피 주소와 변환할 수 없는 포트 주소를 이용한랜 네트워크 주소 변환 게이트웨이

요약

네트워크 주소 변환 게이트웨이는 로컬 IP 주소들을 사용하는 근거리 네트워크로부터 외부 네트워크로 전송하는 IP 데이터그램에 대한 일반 네트워크 변환을 제공하나, 포트가 IPSec 프로토콜 모델의 일부분인 ISAKMP '핸드쉐이킹' 프로토콜과 같은 특정 프로토콜에 대해 예약되어 있을 때 소스 주소 (포트) 변환을 중지한다. ISAKMP 변경은 동일 서비스 주소를 사용하는 소스 및 타겟 컴퓨터들을 필요로 한다. 소스 서비스 주소(포트)를 변환하지 않는 네트워크를 제공함으로써 본 게이트웨이는 로컬 IP 주소들을 사용하는 로컬 에어리어 네트워크와 인터넷 상의 서버들 사이에서 사용하는 안전하고 암호화된 변환의 초기화 및 유지를 가능하게 한다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 로컬 IP 주소들을 이용하는 원격 랜에서의 가상 사설 망이 인터넷과 같은 외부 네트워크를 통하여 메인 컴퓨팅 사이트와 네트워크되어 있는 것을 도시한 것이다. 랜은 NAT 게이트웨이를 통하여 외부 네트워크에 연결되어 있다.

도 2는 인터넷으로 전송하기 위한 랜으로부터 수신한 UDP 데이터그램들을 프로세스하기 위해 본 발명의 게이트웨이에 의해 사용된 결정 차트를 도시한 것이다.

도 3은 랜 상의 장치로 전송을 위해 인터넷으로부터 수신한 UDP 데이터그램들을 프로세스하기 위해 본 발명의 게이트웨이에 의해 사용된 단계들의 결정 차트를 나타낸다.

도 4는 도 5, 도 6 및 도 7에 도시된 차트들에서의 참조를 위해 제공된 것이다. 도 4는 랜(L-1부터 L-3) 상의 로컬 장비들의 IP 주소들, 게이트웨이의 내부 및 외부 IP 주소들 및 외부 네트워크 상의 외부 장치들('타겟' T-1부터 T-3)의 IP 주소들을 포함하는 테이블이다.

도 5a 내지 도 5c는 랜(L-1, L-2,... ,L-X) 상의 장비들의 로컬 IP 주소들과, 외부 장치들(T-1부터 T-3)의 외부 IP 주소들을 암호화된 데이터그램들을 확인하는데 사용된 SPIs(보안 파라미터 인덱스들)과 상호 참조하는 게이트웨이의 내부 테이블로부터의 대표적인 필드들을 나타낸다. SPI-In이 랜 상에서 로컬 장비를 목적지로 하는 암호화된 데이터그램의 SPI를 나타내는 한편, SPI-Out은 인터넷 상의 장치들을 향해 게이트웨이를 떠나는 암호화된 데이터그램의 SPI를 나타낸다. 테이블의 각각의 뷰(view)(a), (b), (c)는 상이한 시점들에서 소스, 목적지, 및 SPI에 대한 헤더 값들을 반영한다. 변경 값들은 타겟 장비와 함께 하나의 로컬 장비에 의하여 새로운 세션의 개시를 의미한다.

도 6은 하나의 로컬 장비와 외부 네트워크 상의 하나의 장치 사이에서 교환된 데이터그램 헤더들 내의 대표적인 필드를 나타낸다. 헤더 값들은 본 발명의 게이트웨이에 의한 프로세싱을 거쳐 변경된다.

도 7은 본 발명의 게이트웨이에 의한 프로세싱을 거쳐 수정된 바와 같이, 랜 상의 3개 로컬 장비(L-1부터 L-3)과 외부 네트워크 상의 3개 타겟들(T-1부터 T-3) 사이에서 교환된 데이터그램 헤더들내의 대표적인 필드들을 나타낸다.

도 8은 데이터그램 프로세싱 기능과 타이머 사이에서 전달되는 신호들의 개략적인 다이어그램이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

TCP/IP(Transfer Control Protocol/Internet Protocol)을 이용하는 가상 사설 네트워킹(Virtual Private Networking :VPN)은 통신 매체로서 인터넷을 이용하는 컴퓨팅 사이트간에 보안 및 빠른 속도의 통신을 가능하게 한다. 인터넷을 통해 양 사이트간에 전달되는 정보는 다양한 보안 수단에 의해 악의의 해커 또는 요구되지 않은 도청자들에 의한 가로채기로부터 보호된다. 효과적인 보안 수단은 최소한 다음의 사항들의 일부 또는 전부에 대한 보호를 보장할 수 있는 기술들을 결합하여야 한다: 전송 중에 악의 또는 부주의에 의한 데이터 변경으로부터 데이터 보전; 복제 금지 수단을 사용함으로써 서비스 거부 공격 방해; 소스(Source) 인증; 전송 중 소스 주소 또는 다른 헤더 정보의 비밀 유지; 요구되지 않은 가로채기로부터 패킷 페이로드 보호. 인터넷 보안을 제공하는 하나의 표준적인 모델은 IPSec(Internet Protocol Security suite)이다. IPSec은 인터넷에 연결된 장치 또는 인터넷에 연결된 사설 랜간의 통신 보안을 제공하기 위해 TCP/IP 통신 프로토콜과 함께 동작한다.

TCP/IP 프로토콜은 네트워크상에서 각 장치를 식별하는 IP(Internet Protocol) 주소를 사용한다. 범용의 IP 주소는 인터넷상의 어떠한 장치를 유일하게 식별한다. 이러한 장치는 컴퓨터, 프린터, 라우터, 스위치, 게이트웨이 또는 기타의 네트워크 장치들일 수 있다. 범용의 IP 주소를 가지는 장치는 인터넷상에서 직접 소스 또는 목적지가 될 수 있다. 그러나, TCP/IP 통신 프로토콜이 오직 인터넷에 제한되는 것은 아니고 사설 랜에도 이용될 수 있다. TCP/IP를 사용하는 사설 랜은 네트워크 장치에 대해 로컬 IP 주소를 많이 이용한다. 사설 랜의 두 장비가 같은 로컬 IP 주소를 공유하지는 않더라도, 사설 랜은 인터넷과 격리되어 있으며, 랜에 있는 로컬 장치를 인터넷으로부터 볼 수는 없다. 그러므로, 로컬 장치의 IP 주소는 범용의 독자적인 IP 주소일 필요가 없다. 로컬 IP 주소를 사용하는 랜은, 랜과 인터넷간의 메시지를 라우팅하고 필터링하는 장치인 게이트웨이(Gateway)를 통해 인터넷과 연결된다. 게이트웨이가 직접적으로 인터넷에 연결되고 인터넷에서 볼 수 있기 때문에, 게이트웨이는 인터넷을 통해 통신할 수 있는 범용의 독자적인 IP 주소가 있어야 한다. 그러나, 랜은 인터넷으로부터 직접적으로 보이기 않기 때문에, 랜에 있는 로컬 장치는 범용의 독자적인 IP 주소를 요구하지는 않는다.

TCP/IP는 인터넷에서 사용되는 통신 프로토콜이다. TCP/IP를 이용하여 통신할 정보는 '데이터그램(Datagram)'에 포함되어있다. 데이터그램은 하나 또는 그 이상의 헤더가 덧붙여진 정보의 불연속적인 패킷으로 구성된다. 헤더는 TCP/IP에 의해 패킷을 의도하는 목적지로 전송하고 전송 중에 적절한 처리를 보장하는데 필요한 정보를 포함한다. 각 데이터그램은 주소에 의해 지시할 수 있는 것이고, 접속 지향적인 TCP 데이터그램일 수 있으며 또는 접속이 유지되지 않는 UDP(User Datagram Protocol)일 수 있다. 각 UDP 데이터그램은 IP 헤더와 UDP 헤더를 포함한다. UDP 헤더가 소스와 목적지 서비스 주소(포트 주소, 번호로 주어짐)를 포함하는 반면에, IP 헤더는 최소한 '소스' IP 주소와 '목적지' IP 주소를 포함한다. IP 버전4 에서, IP 주소는 32비트의 길이를 가지며, 이제는 익숙한 xxx.xxx.xxx.xxx 형태로 결합된다. 이러한 형태에서, 각 세 개의 디지트 세그먼트(Segment)는 0부터 255를 나타내는 바이너리 옥텟(Octet)이다. 완전한 IP 주소는 로컬 네트워크 또는 네트워크 세그먼트와 네트워크상의 '노드'(장치)의 주소를 결합한다. 네트워크 또는 네트워크 세그먼트의 주소는 첫 번째 3,6 또는 9의 IP 주소 디지트를 포함할 수 있다. 네트워크 또는 네트워크 세그먼트상의 장치는 네트워크 또는 네트워크 세그먼트 주소에서 사용되지 않고 남아있는 디지트로 구성되는 노드 어드레스에 의해 식별된다.

UDP 헤더에 포함되어 있고, '포트' 또는 '소켓' 등으로 알려진 소스와 목적지 서비스 주소는 16비트 넘버이며, 패킷을 수신중 도는 송신중인 장비에서 진행중인 의도한 프로세스로 전송한다. 여기서 사용되는 '포트' 또는 '포트 주소'라는 용어는 UDP 헤더에서 서비스 주소 필드를 말한다. 이론적으로 16비트 넘버로 구성될 수 있는 많은 주소가 있기는 하지만, 현실적으로 많은 포트 주소가 정해진 프로세스를 위해 예약되어 있다. 즉, 예를 들어, 포트 80은 HTTP를 위해 예약되어 있으며, 포트 20과 포트 21은 FTP를 위해 예약되어 있다. 포트 주소를 사용함으로써, 하나 이상의 프로세서를 구동하고 있는 장치로 도착한 데이터는 데이터가 의도하는 프로세스로 전달될 것이다. 로컬 호스트에서 진행하는 프로세스가 예약된 프로세스 중 하나가 아닐 경우, 로컬 호스트는 '소스' 프로세스를 식별하기 위해 예약되지 않은 포트 번호를 선택할 수 있다. '목적지'에서 그 포트 번호를 가리키는 응답 패킷이 프로세스로 전달될 것이다.

지난 10년간 인터넷 사용의 폭발적인 증감 및 앞으로의 계획된 성장에 비추어볼 때, 범용의 독자적인 IP 주소는 점차 고갈되고 있다. 사설 랜을 유지하는 많은 비즈니스는 랜 상의 각 컴퓨터와 장치가 범용의 독자적인 IP 주소를 가지게 할 필요가 없다. 어떠한 경우에, 많은 비즈니스는 컴퓨터 IP 주소에 대해 비밀이 유지되는 것을 선호한다. 각 로컬 장치에 범용의 독자적인 IP 주소를 줌으로써, 제한된 범용 자원을 낭비하기보다, 많은 사설 랜은 랜 상의 장치에 로컬 IP 주소를 이용한다. 인터넷과의 연결을 제공하기 위해 그러한 랜은 랜과 인터넷을 분리하는 게이트웨이에 의해 인터넷에서 이용될 범용의 독자적인 주소를 사용한다.

네트워크 주소 변환(Network Address Translation : NAT) 기술을 이용함으로써, 랜과 인터넷을 분리하는 게이트웨이는 방화벽으로서 보안을 제공할 수 있고, 로컬 IP 주소를 가진 장비로 하여금 게이트웨이의 범용의 독자적인 IP 주소를 통해 인터넷에 액세스할 수 있도록 한다. 랜의 장치는 고정 IP 또는 유동 IP를 가질 수 있다. 게이트웨이는 랜에 있는 각 장치의 로컬 IP 주소에 대한 변환 테이블을 가지고 있다. 로컬 장비로부터 전송되고 인터넷이 목적지인 UDP 패킷은 IP와 UDP 헤더의 소스 필드에서 식별되는 로컬 IP 주소와 포트 주소를 가질 것이다. 게이트웨이는 로컬 장비로부터 패킷을 수신하고, IP와 UDP 헤더의 소스 필드를 게이트웨이의 범용의 독자적인 IP 주소 및 새로운 포트 주소(사용되지 않거나 예약되지 않은 포트 주소)로 대체한다. 그 후, 게이트웨이는 CRC(Cyclical Redundancy Check)를 갱신하고 데이터 보전을 위해 필요한 다른 어떤 변화를 수행하며, 그 후 패킷을 인터넷으로 전송한다. 프로세서의 일부로서, 게이트웨이는 장비에 의해 최초로 보고되는 소스 포트 주소를 가진 IP 주소와 인터넷에 구속된 패킷에 할당된 새로운 포트 주소 및 목적지 IP 주소를 상호 참조할 수 있도록 내부의 변환 테이블을 갱신한다. 인터넷으로부터 응답을 수신할 경우, 게이트웨이는 패킷 헤더에서 고유의 IP 주소를 인식하고 들어오는 패킷의 목적지 포트 주소를 조사한다. 만약 게이트웨이가 목적지 포트 주소를 내부의 테이블에서 발견하면, 게이트웨

이는 패킷의 목적지 필드를 상호 참조된 로컬 장비의 IP 주소와 최초의 포트 주소로 대체하고, CRC와 다른 필요한 파라미터를 갱신하며, 패킷을 랜으로 전송한다. 랜에서 패킷은 로컬 장비로 수신되고 적절한 프로세스에 지정된다. 이러한 방법으로 랜에 있고 로컬 IP 주소만을 가지는 컴퓨터가 하나의 범용의 독자적인 IP주소를 통해 인터넷으로 통신을 할 수 있다.

NAT 게이트웨이가 인터넷으로부터 직접적인 랜 액세스에 대비한 방화벽 보안을 제공할지라도, 인터넷상에서 랜으로 전송중의 패킷의 변경이나 가로채기에 대한 보안을 제공하지는 못하며, 랜 내부에서 생기는 공격으로부터 신용을 보장하지 못한다. 그러므로, IPSec에 의해 제공되는 보안은 인터넷과 인터페이싱 중에 보안을 유지하여야 하는 랜의 보호를 위해 필요하다. 일반적으로 IPSec는 하나 이상의 메인 컴퓨팅 사이트와 하나 또는 그 이상의 격리된 LAN으로 구성되는 가상 사설 네트워킹(VPN)에 대한 보안을 제공한다. 고가의 사설 대여망을 대신하고 사이트간의 통신을 위한 고속의 매체인 인터넷을 통해 메인 사이트와 격리된 랜은 연결되어 있다. 전송 매체로서 인터넷을 사용할 경우의 문제점은 인터넷이 본래 안정적이지 못하고 해커에 의한 염탐, 감지, 속임수 또는 절취, 메시지의 변경 또는 전환에 대해 보호를 받지 못한다는 것이다. 따라서, 안전한 데이터 전송이 요구되는 포괄적인 보안 수단이 필요하다. IPSec 프로토콜은 데이터와 데이터 보전의 인증을 보장할 수 있는 보안 수단으로서의 요건을 충족시킨다.

IPSec 프로토콜은 다층의 OSI(Open Systems Interconnection) 네트워크 참조 모델의 네트워크 층에서의 보안을 수행한다. 이는 인터넷을 통해 정보를 전달하는 UDP 데이터그램의 보안을 보장하도록 서로 연결되어 사용되는 다수의 분리된 프로토콜을 포함한다. IPSec에 따른 시스템의 기본적인 구조는 RFC2401, '인터넷 프로토콜을 위한 보안 구조(켄트, R.앳킨슨; 1998년 11월)'에 설명되어 있다. 인증 헤더(Authentication Header : AH) 프로토콜은 데이터 보전 및 소스 인증을 보장하고 서비스 거부 공격을 막는 '복사-금지(anti-repeat)'를 실시한다. ESP(Encapsulation Security Payload) 프로토콜은 인증 헤더와 유사한 보호 기능을 제공하나 페이로드 암호화라는 부가적인 특징이 있다. 인증 헤더와 ESP 헤더는 모두 보안 파라미터 인덱스(Security Parameter Index : SPI)를 위한 필드를 가지고 있다. 보안 파라미터 인덱스는 데이터그램에 대한 보안 조합(Security Association : SA)을 식별하는 32비트의 의사-랜덤(Pseudo-random) 값이다. 나아가, 이러한 프로토콜에 관계된 정보는 RFC1826 'IP 인증 헤더(R. 앳킨슨, 1995년 8월)' 및 RFC2406 '보안 페이로드를 캡슐화하는 IP(S. 켄트, R. 앳킨슨; 1995년 8월)'에서 찾을 수 있다.

ISAKMP/Oakley (Internet Security Association and Key Management Protocol, 일반적으로 인터넷 키 교환이라고 알려짐)는 두 호스트간의 보안 세션(Session)을 위한 파라미터를 설정하고 키 및 보안 세션을 실행하고 암호화된 데이터 전송을 허락하는데 사용되는 기타의 보안 정보의 교환을 제공하는 신호 변경(Handshaking) 프로토콜이다. ISAKMP/Oakley 프로토콜(이하 'ISAKMP'라 함)은 인증이 이루어지고 데이터 암호화를 위한 보안키가 발생되는 초기 데이터를 두 장비 모두에 제공하기 위해 암호화되지 않은 메시지의 초기 교환을 포함한다. 이러한 프로세서들에 관한 설명은 RFC2409, '인터넷 키 교환(D. 하킨스, D. 캐럴; 1998년 11월)'에서 찾을 수 있다. 보안 조합(SA)을 개설하기에 충분한 보안 파라미터가 호스트간에 교환되면, 그 후의 모든 전송은 동의된 프로토콜에 따라 암호화되고 전체적으로 인증된다. 그 시점에서 ISAKMP 프로토콜은 종료한다. 그 후의 어드레싱은 각 장비의 IP 주소와 그 세션을 위한 장비의 SPI에 기초한다. SPI는 한 세션 동안에 각 장비에 있어서 유일하다. 사설 랜을 위한 게이트웨이는 내부의 테이블을 유지한다. 상기 테이블에서, 'SPI-in' 은 로컬 장비의 IP 주소와 상호 참조되고, 'SPI-out'은 로컬 장비와 통신하고 있는 인터넷 장비의 IP 주소와 상호 참조된다. 각 장비의 SPI는 ISAKMP 전송중에 교환된 정보로부터 계산되고, UDP 패킷에 부가되는 인증 또는 ESP 헤더에 실린다. IPSec 프로토콜은 다양한 환경에서 보안을 제공할 수 있기 때문에, 하나의 데이터그램이 인증 헤더와 ESP 헤더를 모두 포함하고 헤더 정보를 암호화할 수 있다.

전술한 보안 프로토콜들 각각은 새로운 헤더 정보를 패킷에 부가하고, 사용되고 있는 프로토콜에 맞도록 패킷 내의 특정 필드를 변경하고, 어떤 경우에는 페이로드와 다른 패킷 헤더의 전부 또는 일부를 암호화함으로써 UDP를 변경한다. 따라서, IPSec하에서, UDP 데이터그램이 전송을 위해 보안이 보장되지 않은 네트워크를 통해 보안된 도메인을 출발할 경우, UDP 데이터그램은 일반적으로 IP 헤더, 인증 헤더 또는 ESP 헤더(또는 인증헤더와 ESP 헤더 모두) 및 캡슐화된 페이로드로 구성될 것이다. 헤더 정보는 데이터그램이 목적지에 도착하고 목적지 호스트에서 인증될 수 있도록 목적지 주소, SPI, 충분한 SA 정보를 포함한다. 페이로드의 캡슐화는 페이로드에 포함된 정보에 요구되지 않은 도청자나 해커가 진입하는 것을 막을 수 있도록 한다. 데이터그램에 대한 초기의 목적지 호스트는 라우터, 게이트웨이 또는 랜과 인터넷사이의 방화벽일 수 있다. 랜과 인터넷 사이의 경계에 있는 장치에 도착 시, 데이터그램은 열리고, 조사되거나 전부 또는 일부가 복호화되며, 상세한 주소 정보를 위해 분석되고, 랜의 로컬 IP 주소로 라우팅된다.

IPSec에 사용되는 ISAKMP 핸드쉐이킹(Handshaking) 프로토콜은 보안 세션을 설정하는 두 호스트간에 프로세스가 특정된 포트 주소(포트 500)를 초기의 메시지 교환을 위해 사용할 것을 요구한다. 이러한 이유로 인해, 포트 500은 ISAKMP 프로토콜에 독점적으로 사용되도록 할당되어 있다. 일반적으로 ISAKMP 프로토콜을 이용하여 보안 통신 파라미터에 대한 협상을 시도하는 컴퓨터는 엄밀히 각 컴퓨터의 포트 500을 통해 통신하여야 한다. 즉, 각 컴퓨터로부터의 ISAKMP 메시지는 소스 및 목적지 포트 주소로 포트 500을 식별하여야 한다. 만약 어떤 컴퓨터가 소스 및 목적지 주소로 포트 500이 특정되지 않은 패킷을 수신할 경우에, 그 패킷은 버려진다.

이 프로토콜이 두 호스트가 서로 통신을 하고 있다는 것을 보장하는 반면에, 어느 한 호스트가 로컬 IP 주소와 NAT 게이트웨이를 사용하고 있는 랜에 위치할 경우에는 사용할 수 없게 된다. 예를 들어, NAT 게이트웨이에 의해 보호되는 격리된 랜에서 로컬 IP 주소를 가진 호스트 A가 메인 오피스 컴퓨팅 사이트에 위치한 호스트 B와 보안 세션을 설정하고자 한다고 하자. 호스트 A는 암호화되지 않은 UDP 데이터그램을 호스트 B로 전송하고 목적지로 호스트 B의 IP 주소를 주며 목적지 포트 주소로 포트 500을 줌으로써 프로토콜을 초기화한다. 그러나, 데이터그램이 격리된 랜을 인터넷에 연결하는 NAT 게이트웨이에 도착할 때, 게이트웨이는 목적지 포트 주소를 임의의 포트 번호로 변환할 것이다. 데이터그램이 호스트 B에 도착할 때, ISAKMP 프로토콜은 인식되지 않고, 호스트 B는 응답하지 않을 것이다. 컴퓨터들은 보안 세션을 설정하는데 실패한다. 이러한 어려움 때문에, 격리된 랜에 있는 각 컴퓨터가 범용의 IP 주소가 아닌 로컬 IP 주소를 사용할 경우, ISAKMP 프로토콜은 NAT 게이트웨이를 이용한 가상 사설 네트워킹(VPN)을 설정하는데

사용할 수 없다고 생각되어 왔다.

발명이 이루고자하는 기술적 과제

본 발명의 목적은 인터넷을 통신 매체로 사용하는 호스트 컴퓨터와 범용의 IP 주소를 사용하지 않는 컴퓨터간의 ISAKMP 프로토콜 인증 및 키 교환을 가능하도록 하는 게이트웨이를 제안하는 것이다.

본 발명의 또 다른 목적은 로컬 IP 주소를 사용하는 사설 랜의 어떠한 수의 컴퓨터라도 ISAKMP 프로토콜을 이용하여 인터넷을 경유해 메시지를 초기화하고 수신하도록 하는 게이트웨이를 제안하는 것이다.

본 발명의 또 다른 목적은 안전한 통신을 초기화하기 위해 ISAKMP 프로토콜을 이용하여 인터넷상의 두 개 이상의 랜 사이트간에 가상 사설 네트워킹을 사용하는 방법을 제안하는 것이다.

발명의 구성 및 작용

본 발명에 따르면, NAT 게이트웨이를 통하여 인터넷과 같은 외부 네트워크에 연결되어 원격 랜상에서 로컬 IP 주소를 사용하는 컴퓨터는 키들을 교환하고, IPSec 하에서 보안 세션을 지원하는 SAs를 확립하기 위하여 ISAKMP 프로토콜을 사용할 것이다. non-ISAKMP 트래픽을 위하여, 게이트웨이는 일반적인 주소 변환을 수행한다. 그러나, 랜상에 장비는 ISAKMP 프로토콜 메시지가 발생할 때마다, 게이트웨이는 포트 500의 포트 주소를 포함하는 데이터그램을 확인한다. 이러한 데이터그램을 확인할 경우, 게이트웨이는 소스 IP 주소를 변환하지만, 소프 포트 주소는 변환하지 않고 포트 500에 남겨두고, 소스와 도착지 포트 주소 모두가 지정된 포트 500을 사용하여 인터넷에 패킷을 보낸다. 또한, 게이트웨이는 내부 테이블을 포트 500을 구속하기 위하여 업데이트하고, 그 구속을 미리 지정된 시간동안 목적지 장비의 외부 IP 주소와 연관시킨다. 미리 지정된 시간 내에 유효한 응답이 도착되지 않으면, 포트 500과 로컬 IP 주소 사이의 구속이 해제된다. 이러한 특징은 예를들어, ISAKMP 프로토콜 전송이 정확하지 않은 목적지 IP 주소에 초기화되어진 경우에, 포트 500이 막연히 구속되어 있지 않는다는 것을 보증하는데 필요하다. 이러한 조건하에서 게이트웨이는 유효한 응답을 결코 수신하지 않을 것이다. 유효한 응답이 수신되지 않는 기간이 경과한 후에 포트 500을 해제하기 위한 타이머가 없다면, 그 포트는 게이트웨이가 리셋될 때까지, 로컬 IP 주소에 구속되어 있을 것이다. 대부분의 경우에 있어서, 2초 동안의 시간은 유효한 응답을 기다리기 위해 포트 500과 로컬 IP 주소 사이의 구속을 유지하기 위한 충분한 시간일 것이다.

포트 500이 로컬 IP 주소에 구속되어 있는 시간 동안, 유효한 응답을 대기하면서, 게이트웨이는 포트 500 포트 주소를 가지고 있지 않는 데이터그램의 통상적인 데이터그램 처리를 진행할 것이다. 유효한 응답은 포트 500에 관계된 외부 IP 주소와 같은 소스 IP 주소를 가지고 있는 데이터그램이고, 소스와 목적지 포트 주소가 모두 포트 500이다. 유효한 응답을 기다리는 동안 게이트웨이는 포트 500 소스와 목적지 포트 주소를 가지고 있는 외부 네트워크로부터의 다른 UDP 데이터그램들을 무시하지만, 적절한 소스 IP 주소의 경우에는 그러하지 아니하다. 또한, 포트 500이 로컬 IP 주소를 구속하는 동안, 포트 500의 소스와 목적지 포트 주소를 가지고 있는 랜으로부터 수신된 데이터그램에 대해서는 포트 500 소스 포트 주소가 임의로 변환되고, 외부 네트워크에 보내지기 전에 포 사용하지 않는 포트 주소가 되는 일반 주소 변환이 진행된다. 이러한 데이터그램은 포트 500의 소스와 목적지 포트 주소를 가지고 있지 않기 때문에, 유효한 ISAKMP 데이터그램이 아니며, IP 목적지에 도착이 되면 무시될 것이다. 만약, 포트 500을 로컬 IP 주소에 구속하는 기간이 게이트웨이에 유효한 데이터그램이 수신되지 않고 종료되면, 구속은 해제되고 포트 500은 포트 500 소스와 목적지 포트 주소를 가지고 있는 다음 데이터그램에 의해 사용 가능하게 될 것이다.

포트 500이 구속되는 동안, 포트 500의 소스와 목적지 포트 주소 및 정확한 소스 IP 주소를 가진 유효한 응답 데이터그램을 수신할 경우, 게이트웨이는 로컬 장비의 IP 주소를 데이터그램 헤더의 목적지 IP 주소 필드로 대체하면서 데이터그램을 처리하고, 로컬 장비로의 전송을 위해 랜을 통하여 데이터그램을 전송할 것이다. 데이터그램이 게이트웨이를 떠날 때, 게이트웨이는 로컬 IP 주소와 포트 500 사이의 구속을 해제할 것이고 통상적인 데이터그램 프로세싱을 재개할 것이다.

만약, 적절한 소스 IP 주소와 포트 500의 포트 주소들을 가진 응답이 외부 네트워크로부터 수신되지 않으면, 게이트웨이는 기설정된 짧은 시간이 지난 후에 타임아웃될 것이다. 만약 게이트웨이가 유효한 응답을 수신하기 전에 타임아웃이 된다면, ISAKMP 메시지 변환은 완전히 이루어질 수 없고, 재 초기화되어야만 한다.

ISAKMP 프로토콜이 완전히 이루어지고, 부호화된 보안 세션이 진행중일 경우, 게이트웨이는 입력 및 출력 데이터그램들의 ESP 헤더 내부에 있는 SPI를 참조함으로써 로컬 주소 변환을 수행한다. 또한, 게이트웨이는 각각의 패킷 형식(ESP 패킷을 위한 형식 50)이 게이트웨이를 통해 패스되는 데이터그램에 대해 정확하다는 것을 보장할 것이다. 때때로, VPN을 통한 보안 세션은 방해를 받거나, 새로운 세션이 시작되어진다. 이러한 경우에 대한 게이트웨이의 첫 번째 조치는 IP 주소는 인식되나 목적지와 관계된 SPI는 내부 테이블에 나타나지 않는 형태 50 데이터그램의 수신일 것이다. 이러한 경우가 발생할 때, 게이트웨이는 새로운 SPI를 사용하는 목적지 IP 주소에 데이터그램을 전송하고, 또한 목적지 SPI 값(전송 방향에 따라SPI-in 또는 SPI-out)을 게이트웨이의 새로운 테이블에 설정하며, 소스의 SPI 값을 0으로 설정한다. 전송에 대한 응답을 수신할 경우, 게이트웨이는 SPI 필드 테이블에 있는 0을 목적지 IP 주소를 위한 새로운 SPI로 대체한다.

본 발명에 따른 게이트웨이는 메시지를 부호화 또는 복호화 하지 않고, 수신 장비의 프로세싱을 위한 랜 또는 인터넷을 통하여 부호화 또는 복호화되어진 페이로드를 단순히 전송하기 때문에, 집중적인 프로세싱 기능을 요구하지 않고, 비용과 설정의 단순함이 및 유지보수가 중요한 사설 랜에 사용될 것이다.

도 1에서는 사설 랜(10)이 인터넷(50)에 위치한 컴퓨팅 사이트(30)에 연결된 가상 사설 네트워크(VPN)가 도시되어 있다. 랜(10)은 로컬 IP 주소들을 사용하고 본 발명인 네트워크 주소 변환 (NAT) 게이트웨이(20)를 통하여 인터넷에 연결되어 있다. 컴퓨팅 사이트(30)는 비즈니스 본부들, 또는 다국적 단체에 의해 사용되는 많은 수의 사설 네트워크들중 하나, 교육기관, 원격지로부터 자주 액세스되는 다른

어떤 사이트이다. 그런 사이트들은 일반적으로 부호화나 다른 보안 응용을 수행할 수 있는 방화벽이나 게이트웨이(35)를 갖는다. 그런 게이트웨이는 패킷을 열거나, 그것의 컨텐츠를 액세스하거나, 복호화하는 능력을 가지고, 주소 변환, 라우팅, 비캡슐화 그리고 데이터 취급 기능들을 수행한다. 이러한 장치들이 ISAKMP와 다른 IPSec 프로토콜들을 지지할 수 있는 한, 그런 장치들이 패킷을 열고 복호화하고 데이터를 취급함으로써 그렇게 지지하고, 그런 장치들은 메인 컴퓨팅 사이트와 더불어 VPN을 설정하는데 필요로 하는 원격 랜 사이트들 상에서 효과적으로 적용하기에는 너무 비싸고 전력소모가 크다.

메인 사이트의 서버(40)는 VPN 서버 소프트웨어를 실행한다. 원격 사이트의 컴퓨터들(15) 각각은 컴퓨터 상의 IPSec 보안 프로토콜들을 실행하는 VPN 클라이언트 소프트웨어를 각각 실행한다.

랜(10)상의 컴퓨터(15)는 컴퓨팅 사이트(30)의 서버(40)에게 IP 데이터그램을 전송함으로써 게이트웨이(20)를 통해 인터넷 상에서 또는 인터넷을 경유하여 통신한다.

게이트웨이(20)에서 수신한 데이터그램들은 도 2와 도 3에 도시된 결정 차트들에 따라 프로세스된다. 도 2와 도 3의 플로우 차트가 프로세싱 단계들과 상기 단계들을 위한 순서를 나타내고 있을지라도, 일부 기능들을 수행하기 위한 순서가 엄격하지 않고, 일부 단계들은 궁극적인 결과에 영향을 주지 않으며 상기 플로우차트에 도시된 것 이외의 순서로 수행될 수 있다. 예를 들어, 도 2와 도 3은 데이터그램이 게이트웨이에 의해 수신된 후의 첫 번째 스텝이 데이터그램 타입을 결정하는 스텝이고, 마지막 스텝이 데이터그램이 게이트웨이를 통해 전송되기 전에 필요한 IP 주소 변환을 수행하는 스텝을 나타낸다. 하지만, 몇몇 실시예들은 어드레스 변환의 스텝을 프로세스내의 초반의 일부 포인트에 배치하는데, 이는 프로세스의 결과에 영향을 미치지 않는다. IP 주소를 변환하는 순서는 전반적인 프로세스에 있어서 결정적이지 않기 때문에 그 변환이 이루어져야만 하는 시점의 결정은 공학적인 선택의 사안이다.

도 2에 도시된 바와 같이, 랜으로부터 데이터그램을 수신함에 따라, 게이트웨이는 데이터그램이 암호화되어 있는지 아닌지를 보기 위하여 체크한다. 이는 랜이 취급하는 데이터그램의 형식을 결정하기 위해서 그리고 데이터그램이 암호화되어져 있는지 아닌지를 보기 위해 IP 헤더 내의 다음의 헤더 필드를 체크함으로써 수행된다. ESP(50)의 데이터그램 형식은 데이터그램이 암호화되어있고 포트 주소 정보가 사용 가능하지 않음을 나타낸다.

도 2의 결정 트리를 계속 통과하면서 만약 데이터그램이 암호화되어 있다면 게이트웨이는 그것이 게이트웨이 내부 테이블의 SPI-Out 필드내에 나타나 있는지 아닌지를 보기 위하여 데이터그램의 SPI를 체크한다. 그런 테이블로부터의 대표적인 필드들이 도 5a 내지 도 5c에 도시되어 있다. 만약 데이터그램의 SPI가 내부 테이블의 SPI-Out 필드에 발견된다면, 게이트웨이는 데이터그램의 소스 IP 주소를 게이트웨이의 외부 IP 주소가 되도록 변경하고, 외부 장치로 전송하기 위한 외부 네트워크로 데이터그램을 전송한다.

데이터그램이 암호화되어 있고, SPI가 게이트웨이의 내부 테이블에 나타나지 않는다면, 도 2의 결정 차트에 따라 게이트웨이는 데이터그램이 새로운 세션을 초기화하고 있다고 가정한다. 이러한 경우에 게이트웨이는 내부 테이블의 SPI-In 필드를 제로(0)로 설정하고, SPI-Out을 데이터그램으로부터의 새로운 SPI로 설정한다.

이러한, 내부 테이블에 대한 변경들은 도 5a와 도 5b에 반영되어 있는데, 도 5a에서 게이트웨이의 내부 테이블의 SPI-Out 필드에 나타나지 않은 새로운 SPI(14662)는 도 5b에서 SPI-Out 필드에 입력되고, SPI-In이 제로(0)로 설정되도록 도시되어 있다. 암호화된 데이터그램은 이후 소스 IP 주소가 로컬 장치의 IP 주소로부터 게이트웨이의 외부 IP 주소로 변환된 후에 외부 게이트웨이로 전송된다. 이러한 단계들은 도 5b와 도 5c에서 도시되어 있다.

도 2의 결정 차트를 계속 진행하면서 데이터그램이 암호화되지 않았다면, 게이트웨이는 데이터그램의 목적지 포트 주소를 체크한다. 만약 포트 주소가 포트 500을 제외하고 다른 어떤 포트라면, 게이트웨이는 로컬 소스 IP 주소와 상호 참조하여 내부 테이블에 소스 포트 주소를 입력하고, IP 헤더의 소스 주소 필드로 사용하지 않은 임의의 포트 주소를 대체한다. 또한, (로컬) 소스 IP 주소에 상호 참조된 내부 테이블에 새로운 포트 주소를 입력한다. 포트 주소로서 포트 500을 가지고 있지 않는 복호화된 데이터그램들을 위해 사용하는 이런 프로세스는 랜 상에서 발생하는 데이터그램들에 대해 '일반적인 주소 변환'으로 불려진다. 이러한 변환들은 도 6의 1,2번째 줄에 도시되어 있다. 상기 데이터그램은 목적지 IP 주소로 라우팅하기 위한 인터넷으로 보내진다. 도 2에서는 입력되는 데이터그램의 소스와 목적지 포트 주소들이 포트 500이고, 게이트웨이는 포트 500이 이미 IP 주소에 구속되어 있는 지를 보기 위하여 테이블들을 체크한다. 만약, 포트 500이 구속되어있지 않다면, 게이트웨이가 데이터그램의 (로컬) 소스 IP 주소에 포트 500을 구속하고, 포트와 외부 목적지 IP 주소 결합을 생성시킬 것이며, 내부 타이머를 시작하기 위한 신호를 전송한다. 또한, 게이트웨이는 소스 IP 주소 필드내의 로컬 IP 주소를 대신해 게이트웨이의 외부 IP 주소를 사용함으로써 데이터그램을 처리한다. 그러나, 소스 포트 주소를 변환하지 않는다. 소스 포트 주소의 일반적인 변환을 보류함으로써 게이트웨이는 타겟 장비가 데이터그램을 ISAKMP 데이터그램으로 인식할 수 있다는 것을 보증한다. 이러한 단계들은 도 6의 5,6번째 줄에서 나타나 있다.

도 2에서, 만약 랜으로부터 입력되는 데이터그램이 포트 500의 소스와 목적지 포트 주소를 가지고 있으나, 포트 500이 이미 다른 어떤 로컬 IP 주소에 구속되어 있으면, 게이트웨이는 이후 프로세스되는 메시지를 위해 포트 500을 구속할 수 없다. 그러한 경우, 만약 ISAKMP 데이터그램이 아니라도, 게이트웨이는 데이터그램을 일반적으로 프로세스한다. 즉, 데이터그램의 소스 포트 주소를 임의의 숫자로 변환하고, 소스 IP 주소를 게이트웨이의 외부 IP 주소로 변환한다. 게이트웨이는 인터넷에 데이터그램을 보내는데, 상기 데이터그램이 ISAKMP 데이터그램에 일치하지 않기 때문에 타겟에 의해 거절된다. 이러한 경우는 도 7의 15,16번째 줄에 표시되어 있다.

도 3에서, 인터넷으로부터 수신한 프로세싱 데이터그램들에서 게이트웨이가 따르는 단계들을 개략화한 결정 차트가 도시되어 있다. 데이터그램을 수신한 후, 게이트웨이는 데이터그램의 형식을 먼저 체크하고, 만약 데이터그램이 암호화되어 있다면, 데이터그램의 내부 테이블에 SPI가 나타나는지 아닌지를 체크한다. 만약, SPI가 인식되었다면, 그것의 목적지 IP 주소는 로컬 장치의 IP 주소가 되도록 변환되고, 데이터그램은 로컬 장치로 전달되기 위한 랜으로 전송된다. 만약, SPI가 인식되지 않으면, 게이트웨이는 데이터그램의 소스 IP 주소에 해당하는 SPI-In이 제로(0)인지 아닌지를 확인하기 위하여 체크를 한다. 만약,

SPI-In이 제로(0)이면, 게이트웨이는 데이터그램이 새로운 세션의 첫 번째 응답인 것으로 여기고, SPI-In 필드내의 제로(0)를 데이터그램의 SPI-In으로 대체한다. 게이트웨이는 이후, 목적지 IP 주소를 랜 상의 장치의 로컬 IP 주소가 되도록 변환하고, 전송을 위해 랜으로 데이터그램을 전송한다. 이러한 경우가 도 5b와 도 5c에 도시되어 있다. 도 5b에 있어서, 로컬 장비 L-1을 위한 SPI-In은 제로로 설정되어 있다. 게이트웨이가 3288의 SPI를 가지고 있는 인터넷으로부터 데이터그램을 수신할 때, 게이트웨이는 SPI-In 필드내에 SPI를 발견하지 못한다. 게이트웨이는 다음에 SPI-In 필드가 제로(0) 라는 값을 유지하고 있는지 아닌지를 확인하기 위하여 다음을 체크할 것이다. 로컬 장비 L-1에 대한 SPI-In이 제로(0)라고 결정되면, 게이트웨이는 제로(0)를 데이터그램(3288)의 SPI로 대체하고, 랜에 데이터그램을 전송한다. 이는 도 5c에 도시되어 있다.

도 3에서, 만약 인터넷으로부터 데이터그램이 암호화되어 있지 않다면, 게이트웨이는 데이터그램이 500의 포트 주소를 가지고 있는지 아닌지를 확인한다. 만약, 그렇지 않다면, 데이터그램에 대해서 랜 상의 장치의 로컬 포트 주소와 로컬 IP 주소가 데이터그램의 목적지 필드들에 대체되는 것을 의미하는, 외부 네트워크로부터의 데이터그램을 위한 일반적인 주소 변환이 수행될 것이고, 데이터그램은 전송을 위해 랜으로 전송된다. 인터넷으로부터의 데이터그램에 대한 일반적인 주소 변환은 도 6의 3,4번째 줄에 도시되어 있다.

도 3을 다시 참조하여, 만약 데이터그램이 500의 포트 주소를 가지고 있다면 게이트웨이는 다음으로 포트 500이 로컬 IP 주소에 구속되어 있는지 아닌지 그리고 데이터그램의 (외부) 소스 IP 주소와 연관되어 있는지 아닌지를 체크해야만 한다. 만약 그렇다면, 데이터그램은 유효하고, 목적지 IP 주소가 외부 게이트웨이의 IP 주소로부터 로컬 장치의 IP 주소로 변환된 후에 랜으로 전송된다. 데이터그램을 랜으로 전송하면, 게이트웨이는 포트 500을 해제한다. 이러한 경우는 도 6의 7-8번째 줄에 나타나 있다.

만약, 도 3에서 포트 500이 로컬 IP 주소에 구속되어 있고, 데이터그램의 소스 IP 주소 내에 발견된 것 이외의 외부 IP 주소에 연관되어 있다면, 데이터그램은 유효하지 않고 게이트웨이에 의하여 더 이상 프로세스되지 않는다. 이러한 경우는 도 7의 25-31번째 줄에 도시되어 있다. 25,26번째 줄에서는 로컬 장비(L-1)가 ISAKMP 데이터그램을 타겟(T-1)으로 전송한다. 이 때, 포트 500가 로컬 장비(L-1)의 IP 주소에 구속되고, 타겟(T-1)의 IP 주소와 연관된다. 그러나, 도 7에 도시된 바와 같이, 타이머의 타임아웃은 타겟(T-1)으로부터 게이트웨이에 수신되기 전에 종료하고, 27번째 줄에서 포트 500이 해제된다. 28,29번째 줄에서는 로컬 장비(L-3)의 IP 주소에 포트 500을 구속하고 타겟(T-3)의 IP 주소와의 연관을 생성하며, 로컬 장비(L-3)이 타겟(T-3)에 ISAKMP 데이터그램을 전송한다. 포트 500이 구속되어 있는 동안, 응답이 타겟(T-1)으로부터 수신된다. 그러나, 포트 500이 구속되고 타겟(T-3)의 IP 주소와 관계가 있기 때문에 타겟(T-1)으로부터의 응답은 버려진다. 이는 도 7의 30,31번째 줄에 나타나 있다.

도 5a 내지 도 5c는 IP 주소들과 인터넷상의 로컬 컴퓨터들과 타겟들 사이의 암호화된 통신을 위한 SPI 숫자들을 보유하고 있는 게이트웨이의 내부 테이블을 나타내고 있다. (L-1), (L-2), ...,(L-x)와 (T-1) 내지 (T-3)를 위한 필드들은 참조의 편의상 포함되어 있고, 게이트웨이의 내부 테이블들에는 나타나 있지 않다. 도 5에서는 SPI-Out 필드가 랜 상의 특정한 컴퓨터의 보안 세션 동안에 각각의 타겟 장비를 위한 SPI를 유지한다. SPI-In 필드는 유효한 데이터그램을 나타내는 것으로 로컬 컴퓨터에 의하여 인식되어지는 해당 SPI를 제공한다. 도 5a는 초기 시점에서의 테이블을 나타낸다. 8개 로컬 컴퓨터들은 테이블 데이터의 수명 동안에 3개 타겟(T-1 내지 T-3)과 함께 암호화된 세션들에 참여했다. 이는 각 로컬 장비가 IP 주소에 관계된 SPI-In을 나타낸다는 사실에 의해서 나타난다. 비록 단지 3개 타겟들이 테이블에 도시되어 있지만, 각 타겟이 각 로컬 장비와 통신하기 위한 다른 SPI-Out을 사용하고 있다는 것을 주지하여야 한다. 이러한 방식으로, 타겟은 어느 소스로부터 암호화된 데이터그램소스가 생성되어져 있는 가를 알게 된다.

도 5b는 도 5a와 같이 동일한 로컬과 타겟 컴퓨터들을 나타낸다. 하지만, 여기서는, (L-1)과 (T-1) 사이의 세션을 위한 SPI-Out이 컴퓨터들 사이의 새로운 세션을 나타내는 새로운 SPI이다. 새로운 세션이 발생함을 나타내는 게이트웨이의 첫 번째 조치는 테이블에 없는 SPI('14662')을 갖는 랜으로부터 암호화된 데이터그램의 수신이다. 게이트웨이는 인터넷에 데이터그램을 전달하고, 데이터그램을 위한 소스와 목적지 IP 주소들에 관계된 SPI-Out 필드에 새로운 SPI를 배치하기 위해 테이블을 변경한다. 새로운 SPI-In이 기대되는 것을 표시하기 위한 표시자로서 SPI-In 필드에 제로를 배치한다. 도 5c는 새로운 SPI('3288')이 (T-1)으로부터 수신된 데이터그램에 포함되어 있는 것을 나타낸다. 상기 SPI는 게이트웨이의 SPI-In 필드내에 입력되고, 이 세션동안에 (L-1)과 (T-1) 사이의 통신이 그들의 메시지들을 확인하기 위해 SPI들을 사용한다.

도 6은 인터넷상의 원격 타겟과 통신하는 랜 상의 단일 컴퓨터에 의하여 본 발명의 게이트웨이를 통과하는 대표적인 데이터그램의 흐름을 나타낸다. 차트의 각 행은 게이트웨이와의 랜 인터페이스나 게이트웨이와의 인터넷 인터페이스에서의 데이터그램의 정보를 나타낸다. 연속적인 행들은 일측으로부터 게이트웨이에 입력하고, 타측으로부터 게이트웨이를 떠나는 데이터를 나타낸다. 게이트웨이는 랜과의 인터페이스에서 로컬 IP 주소이고, 인터넷과의 인터페이스에서 범용 IP 주소인 하나의 IP 주소를 가지고 있다. 도 6의 열은 데이터그램이 경유하는 게이트웨이의 사이드와 데이터그램의 형태, 데이터그램의 소스 IP 주소와 포트 주소, 데이터그램의 목적지 IP 주소와 포트 주소, ESP 프로토콜을 이용하는 타입(50)의 암호화된 데이터그램들을 위한 데이터그램의 보안 파라미터 인덱스를 나타낸다.

도 6의 1번째 줄은 게이트웨이의 로컬 인터페이스에 도착하고, 로컬 컴퓨터(L-1)에 해당하는 소스 IP 주소와, 인터넷 상의 타겟(T-1)의 목적지 IP 주소를 가지고 있는 UDP 데이터그램을 나타낸다. 읽기의 용이함을 위해 도 4는 로컬 목적지들(L-1 내지 L-3)과 타겟 목적지들(T-1 내지 T-3)에 교차 참조되는 IP 주소들의 테이블을 제공한다. (L-1)을 위한 소스 포트 주소가 포트 6404이고 타겟의 목적지 포트는 포트 80이다. 데이터그램이 암호화되지 않고, 500의 포트 번호를 나타내지 않기 때문에, 데이터그램은 임의의 포트 주소, 포트 10425를 소스 포트 주소 필드로 대체하고 게이트웨이의 외부 IP 주소가 데이터그램의 소스 IP 주소로 대신하는 일반적인 변환이 진행된다. 비록, 변환된 소스 포트 주소는 임의적이라고 하더라도, 일반적으로 게이트웨이에 의하여 유지되는 현재 사용하지 않고 예약하지 않은 포트 주소들의 풀(pool)로부터 얻어진 연속적인 것들이다.

도 6의 2번째 줄에서와 같이, 데이터그램이 게이트웨이를 벗어날 때, 게이트웨이의 주소 변환 기능은 게이트웨이의 외부 IP 주소를 소스 IP 주소를 위한 데이터그램 헤더로 대체하고, 소스 포트에 임의의 번호를 부여한다. 3,4번째 줄은 타겟으로부터의 응답 데이터그램을 나타낸다. 3번째 줄에서는 타겟으로부터의 UDP 데이터그램이 게이트웨이의 외부 IP 주소인 목적지 IP 주소와, 게이트웨이에 의해 임의로 지정된 포트 주소인 목적지 포트를 나타낸다. 데이터그램이 암호화되지 않고 500의 포트 주소를 가지고 있지 않기 때문에 데이터그램에 대해 목적지 포트 주소와 IP 주소의 일반적인 변환을 겪게되고, 이어 랜으로 전송된다. 4번재 줄에서는 게이트웨이가 랜으로 데이터그램을 전송하기 전에 로컬 컴퓨터의 로컬 IP 주소와 포트 주소를 헤더의 목적지 필드안에 대신한다.

도 6의 5번째 줄에서 로컬 컴퓨터는 타겟의 ISAKMP 프로토콜을 초기화한다. 데이터그램 형태는 ISAKMP로서 나타난다. 소스와 목적지 포트 주소는 포트 500이다. 게이트웨이가 목적지 포트 주소가 포트 500이라고 결정할 때, 포트 500이 현재 어떤 IP 주소에 구속되어 있는지 아니지를 확인한다. 그렇지 않으면, 게이트웨이는 소스 포트 주소를 변환하지 않은 채 게이트웨이의 외부 IP 주소를 보이기 위한 소스 IP 주소 필드를 변환한 데이터그램을 전송한다.

도 6의 5-16번째 줄에서는 전적으로 암호화되고 증명된 데이터그램들을 지원하기 위한 보안 조합들(SAs)을 확립하는데 필요한 6개 표준 ISAKMP 핸드쉐이킹 데이터그램 변경을 나타낸다. 비록, ISAKMP의 일부 모드들이 적은 교환을 사용하지만, 메인 모드는 도 6에 나타나 있다. 보안 조합들(SAs)의 확립에 뒤이어, 로컬 컴퓨터와 타겟이 ESP 프로토콜 암호화된 데이터그램들을 사용하여 통신을 시작한다. 여기서, 데이터그램 유효성은 데이터그램의 헤더의 SPI 필드내의 보안 파라미터 인덱스(SPI) 숫자들의 사용을 통하여 유지된다. 각 호스트는 SPI에 주소로 된 데이터그램을 인식하는데, 이는 계속적인 보안을 보장하는데 필요로서 호스트들의 상호 동의에 의해 한 세션동안 변경될 수 있다. 도 6의 17,18번째 줄에 도시된 바와 같이, 암호화된 데이터그램이 게이트웨이를 통해 전송될 때, 비록 데이터그램의 소스 IP 주소가 게이트웨이의 외부 IP 주소로 변환된다고 할지라도 소스나 목적지 SPI 게이트웨이에 의해 변경되지 않는다. 따라서, 암호화된 데이터그램이 게이트웨이에 의해 수신될 때, 형태 50의 데이터그램에 의해 나타난다. 데이터그램의 형태를 볼 때, 게이트웨이는 SPI가 내부 테이블내에 기록되어 있는지 않은지를 알아보기 위해 데이터그램의 보안 파라미터 인덱스(SPI)를 체크한다. 만약, 그렇다면, 게이트웨이는 데이터그램의 소스나 목적지 IP 주소를 적합하게 변환하고, 전송의 방향에 따라, 랜이나 인터넷으로 데이터그램을 전송한다. 하지만, 만약 랜으로부터 데이터그램의 SPI가 게이트웨이의 내부 테이블에 나타나지 않는다면, 그리고 소스나 목적지가 IP 주소들을 인지한다면 게이트웨이는 새로운 세션이 시작된 것으로 여긴다. 이러한 경우, 게이트웨이는 새로운 SPI를 그대로 두나 인터넷 테이블의 SPI-Out 필드에 새로운 SPI를 기록하고, SPI-In 필드에 제로(0)를 대체하는 데이터그램을 외부 네트워크로 전송한다. 행(25),(26)에서는 새로운 SPI가 나타나는, 즉 새로운 세션을 의미하는 것을 도시되어 있다. 이러한 경우는 도 5b에 해당하는데, 'SPI-In' 필드의 0는 14662의 새로운 SPI-Out에 해당한다. 행(27),(28)에서는 외부 네트워크로부터의 응답 패킷은 '이전의' 'SPI 9802'가 '새로운' SPI 3288'로 대치되었음을 나타낸다.

도 7은 본 발명의 게이트웨이를 거쳐 랜 상의 3개 컴퓨터들(L-1), (L-2), (L-3)과 범용의 독자적인 IP 주소들을 갖는 인터넷 상의 3개 타겟들(T1), (T2), (T3) 사이에서 데이터그램 전송을 나타낸 것을 제외하면 도 6과 유사하다. 도 4에는 참조의 편의상 이들 장치들의 IP 주소들을 포함하는 테이블이 주어져 있다. 도 7에 도시된 바와 같이, 'L-1 Out'으로 명기된 송신은 로컬 컴퓨터(L-1)에서 게이트웨이로의 송신을 나타낸다. 'T-1 In'은 게이트웨이에서 타겟(T-1)으로의 송신을 나타낸다. 'T-1 Out'은 타겟(T-1)에서 게이트웨이로의 송신을 나타내고, 'L-1 In'은 게이트웨이에서 컴퓨터(L-1)로의 송신을 나타낸다.

도 7의 1-8번째 줄에 도시된 바와 같이, 컴퓨터들(L-1), (L-2)이 타겟들(T-1), (T-2)과 'in the clear' 통신을 한다. 9번째 줄에서 컴퓨터(L-1)가 타겟(T-1)과 ISAKMP 세션을 시작한다. 8-14번째 줄에서는 ISAKMP 프로토콜 동안에 컴퓨터(L-1)와 타겟(T-1) 사이에서 교환된 첫 번째 3개 메시지를 나타낸다. 15번재 줄에서 컴퓨터(L-3)가 타겟(T-3)과 ISAKMP-1 메시지 교환을 시작한다. 하지만, 이때, 포트 500이 컴퓨터(L-1)에 구속되고 타겟(T-1)의 IP 주소와 연결되어 타겟(T-1)으로부터 ISAKMP-4 응답을 기다린다. 이러한 상태에서는 컴퓨터(L-3)로부터의 데이터그램이 포트500에 구속될 수 없고, 소스 포트 주소가 변환된다. 이 자체만으로 컴퓨터(L-3)가 15번째 줄에서 시작된 송신을 완료할 수 없게 된다.

이 후, 17-18번째 줄에서 타겟(T-1)의 ISAKMP-4 응답이 게이트웨이에서 수신되어 컴퓨터(L-1)로 전송되고, 포트 500이 즉시 가용상태로 된다. 따라서, 컴퓨터(L-3)가 19번째 줄에서 ISAKMP-1 송신을 재시도할 때, 송신이 성공적으로 이루어진다.

도 7의 19-20번째 줄에서 컴퓨터(L-3)의 ISAKMP-1 송신이 포트 500을 컴퓨터(L-3)의 IP 주소에 구속한다. 따라서, 컴퓨터(L-1)가 ISAKMP-5 송신을 시도할 때, 21-22번째 줄에서 포트 500을 사용할 수 없게 되고, 게이트웨이는 단지 포트 500에서 임의의 포트번호(이 경우에서는, 9063)로 목적지 포트 주소를 변환하고 데이터그램을 인터넷으로 송신하는데, 타겟(T-1)이 이를 ISAKMP 데이터그램으로 인식하지는 못한다. 하지만, 컴퓨터(L-3)가 포트 500을 해제한 후 23-24번째 줄에서 ISAKMP-5 송신을 보내는 컴퓨터(L-1)의 다음 시도가 타겟(T-1)에 의해 성공적으로 수신된다. 하지만, 타겟(T-1)의 응답이 느리고, 27번째 줄에서 포트(500)가 컴퓨터(L-1)에 대한 구속으로부터 해제되고, 28-29번째 줄에서 ISAKMP-3 송신을 위한 컴퓨터(L-3)에 의해 즉각적으로 잡혀진다. 따라서, 타겟(T-1)의 ISAKMP-6 응답이 게이트웨이에 도달할 때, 30-31번째 줄에서 도시된 바와 같이, 포트 500이 차단되고, 데이터그램이 무시된다. 이 후, ISAKMP-5 메시지에 대한 응답을 수신하지 못한 컴퓨터(L-1)가 34-35번째 줄에서 이를 재송신하고, 타겟(T-1)으로부터의 응답이 36-37번째 줄에서 수신된다. ISAKMP 핸드쉐이킹에 따르면, 컴퓨터(L-1)와 타겟(T-1)이 38-39번째 줄 및 42-43번째 줄에서 ESP 프로토콜을 사용하여 안전하게 통신할 수 있다.

도 7의 38-57번째 줄은 다수의 로컬 컴퓨터들과 타겟들 사이에서 게이트웨이의 다양한 데이터그램 처리를 나타낸다. UDP 데이터그램은 40-41번째 줄에 나타나 있고, ESP 데이터그램은 42-43번째 줄, 52-53번째 줄에 나타나 있고, 44-45번째 줄에는 ISAKMP 데이터그램이 나타나 있다. 도 7의 차트가 각 장치들에 대한 상이한 IP 주소들을 나타내는 한편, 실제로 다수의 프로세스들이 동일한 장치에서 진행되는 경우가 발생할 수도 있다. 게이트웨이에 의한 독창적인 소스 포트들의 대체와, 암호화된 송신을 차별화하는 SPI의 사용은 하나의 장비에서 진행중인 다중 프로세스들로부터 출력되는 데이터그램이 잘못 지정되지 않도록 보

장하여 준다

도 8은 데이터 프로세싱 회로(100)와 타이머(110) 사이에서 신호의 초기화 및 전송을 나타낸다. IP 주소에 구속될 포트 주소를 필요로 하는 경우가 발생하면, 신호(120)가 타이밍을 시작하기 위해 타이머로 전송된다. 적절한 시간이 지나면, 타이머는 시간이 종료되었음을 나타내는 신호(140)를 전송하는데, 이 경우, 구속된 어떠한 포트도 해제된다. 도중에, 기대한 데이터그램이 도달하고 이전의 구속된 포트가 해제되면, 상기 타이머가 타이밍을 시작하는 다음 신호를 기다리도록 리셋되어야 하는 것을 나타내는 디스에이블 신호(130)가 상기 타이머로 전송된다. 종래의 공지된 다수의 타이밍 회로들이 있고, 도 8에 도시된 특정한 구성은 단지 많은 가능한 실시예들중의 하나이다.

한편, 여기에 기술된 바람직한 실시예가 본 발명을 실시하기 위한 유일한 수단이 아니고, 다른 실시예들이 본 발명의 사상과 영역으로부터 벗어나지 않고 본 발명을 실행하는데 선택될 수 있다는 것은 당 분야의 통상의 지식을 가진 자에게는 자명하다고 할 수 있다. 예를 들어, 바람직한 실시예가 ISAKMP 프로토콜로 사용하는데 독점적으로 예약된 포트 500을 참조하여 기술되어 있을지라도 본 발명은 장래에 다른 프로세스들 또는 프로토콜들에 할당되어질지도 모르는 다른 포트 주소들을 위한 데이터그램들을 프로세싱하는데 동일한 방식으로 적용될 수 있다. 특히, 인터넷을 통하여 이루어지는 많은 게임들은 일반 주소 변환을 감당할 수 없는 로컬 및 외부 장비 상의 특정 포트들의 사용을 필요로 한다. 또한, 본 발명이 사설 랜과 인터넷 사이의 통신에 대하여 주로 기술되었더라도 본 발명의 게이트웨이는 2개 네트워크 사이의 어떠한 인터페이스에서 사용될 수 있고 기술된 바와 같이 동일한 기능을 가짐은 자명하다.

여기에 첨부된 청구범위는 본 발명의 사상과 영역 내에서 수정과 변경을 포함하는 것을 의미한다.

발명의 효과

이상에서 설명한 바와 같이, 본 발명에 의한 게이트웨이에 의하면 인터넷을 통신 매체로 사용하는 호스트 컴퓨터와 범용의 IP 주소를 사용하지 않는 컴퓨터간의 ISAKMP 프로토콜 인증 및 키 교환이 가능하다.

(57) 청구의 범위

청구항 1. 랜을 외부 네트워크에 연결하며, 상기 랜이 로컬 IP 주소들을 사용하고, 상기 게이트웨이가 상기 랜 상의 장치들에 의해 인식할 수 있는 로컬 IP 주소를 가지고 상기 외부 네트워크 상의 장치들에 의해 인식할 수 있는 외부 IP 주소를 가지는 네트워크 주소 변환 게이트웨이에 있어서,

상기 랜 상의 로컬 장치들의 로컬 IP 주소들, 상기 외부 네트워크 상의 외부 장치들의 외부 IP 주소들, SPI-In 값들, SPI-Out 값들, 소스 포트 주소들, 목적지 포트 주소들, 예약된 포트 주소들의 조합들을 결합하고, 예약된 포트 주소들의 리스트를 유지하는 복수개의 내부 테이블들;

상기 랜으로부터 상기 외부 네트워크로 전달되는 데이터그램들과, 상기 외부 네트워크로부터 상기 랜으로 전달되는 데이터그램들에 대해 일반 주소 변환을 수행하기 위한 수단;

상기 외부 네트워크 상의 외부 장치로 전달을 의도하는 상기 랜 상의 로컬 장치로부터 데이터그램을 수신하고, 상기 데이터그램이 암호화되어 있는 지를 결정하고, 상기 데이터그램이 암호화되어 있으면, 상기 데이터그램의 SPI가 상기 내부 테이블의 SPI-Out 필드에 기록되어 있는 지를 결정하고, 상기 데이터그램의 SPI가 상기 내부 테이블의 SPI-Out 필드에 기록되어 있으면, 상기 데이터그램의 소스 IP 주소를 상기 게이트웨이의 외부 IP 주소가 되도록 변경하고, 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하며,

상기 SPI가 상기 내부 테이블의 상기 SPI-Out 필드에 기록되어 있지 않으면 상기 로컬 장치의 로컬 IP 주소에 해당하는 SPI-In 필드를 0으로 설정하고 상기 SPI-Out 필드를 상기 SPI와 동일하게 설정하고, 상기 데이터그램의 상기 소스 IP 주소를 상기 게이트웨이의 상기 외부 IP 주소가 되도록 변경하며, 상기 외부 장치로 라우팅하고 전송하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하고,

상기 데이터그램이 암호화되어 있지 않으면, 상기 데이터그램을 위한 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있는 지를 결정하고, 상기 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있지 않으면, 상기 데이터그램에 대해 일반 주소 변환을 수행하고 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하며,

상기 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있으면, 상기 목적지 포트 주소가 상기 로컬 장치의 상기 로컬 IP 주소에 구속되어 있는 지를 결정하고, 상기 목적지 포트 주소가 상기 로컬 IP 주소에 구속되어 있으면, 상기 데이터그램에 대해 일반 주소 변환을 수행하고 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하고,

상기 목적지 포트 주소가 상기 로컬 장치의 상기 로컬 IP 주소에 구속되어 있지 않으면, 상기 데이터그램의 상기 소스 IP 주소를 상기 게이트웨이의 상기 외부 IP 주소가 되도록 변경하고, 상기 목적지 포트 주소를 상기 로컬 장치의 상기 로컬 IP 주소에 구속하고 상기 목적지 포트 주소와 상기 외부 장치의 상기 외부 IP 주소 사이의 연결을 만들고, 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송함으로써,

상기 랜 상의 로컬 장치로부터 상기 외부 네트워크 상의 외부 장치로 데이터그램을 전달하는 수단;

상기 랜 상의 상기 로컬 장치로의 전달을 의도하는 상기 외부 네트워크 상의 상기 외부 장치로부터 데이터그램을 수신하고,

상기 데이터그램이 암호화되어있는 지를 결정하고 상기 데이터그램이 암호화되어 있으면, 데이터그램의 SPI가 상기 내부 테이블의 상기 SPI-In 필드에 기록되어 있는 지를 결정하고 상기 SPI가 상기 SPI-In 필드에 기록되어 있으면, 상기 데이터그램의 상기 목적지 IP 주소를 상기 로컬 장치의 상기 로컬 IP 주소가 되도록 변경하고 상기 로컬 장치로 라우팅하고 전달하기 위한 상기 랜으로 상기 데이터그램을 전송하고,

상기 SPI가 상기 내부 테이블의 상기 SPI-In 필드에 기록되어 있지 않으면, 상기 외부 장치의 상기 IP 주소에 해당하는 상기 SPI-In 필드가 0인가를 결정하고, 상기 SPI-In 필드가 0이 아니라면, 상기 데이터그램을 버리고,

상기 SPI-In 필드가 0이면, 상기 SPI-In 필드를 상기 SPI와 동일하게 설정하고, 상기 데이터그램의 상기 목적지 IP 주소를 상기 로컬 장치의 상기 로컬 IP 주소가 되도록 변경하고, 상기 로컬 장치로의 전달을 위한 상기 랜으로 상기 데이터그램을 전송하고,

상기 데이터그램이 암호화되어 있지 않으면, 상기 데이터그램을 위한 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있는 지를 결정하고, 상기 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있지 않으면, 상기 데이터그램에 대해 일반 주소 변환을 수행하고 상기 로컬 장치로 전달하기 위한 상기 랜으로 상기 데이터그램을 전송하고,

상기 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있으면, 상기 목적지 포트 주소가 상기 로컬 장치의 상기 로컬 IP 주소에 구속되어 있는 지를 결정하고, 상기 목적지 포트 주소가 상기 로컬 IP 주소에 구속되어 있지 않으면, 상기 데이터그램을 버리고,

상기 목적지 포트 주소가 상기 로컬 IP 주소에 구속되어 있으면, 상기 데이터그램의 상기 목적지 IP 주소를 상기 로컬 장치의 상기 로컬 IP 주소가 되도록 변경하고, 상기 로컬 IP 주소로부터 상기 목적지 포트 주소의 구속을 해제하고, 상기 로컬 장치로 전달하기 위한 상기 랜으로 상기 데이터그램을 전송함으로써, 상기 외부 장치로부터 상기 로컬 장치로 데이터그램을 전달하기 위한 수단을 포함하는 것을 특징으로 하는 네트워크 주소 변환 게이트웨이.

청구항 2. 제 1 항에 있어서,

타이머를 더 포함하고, 포트 주소가 IP 주소에 구속된 신호를 수신하자마자 상기 타이머가 미리 지정된 시간동안 타이밍을 시작하고, 상기 미리 지정된 시간이 종료될 때 상기 포트 주소를 상기 IP 주소로부터 구속되지 않도록 하는 신호를 전송하고, 상기 포트 주소가 상기 미리 지정된 시간의 종료 이전에 상기 IP 주소로부터 구속되지 않은 것을 나타내는 신호를 수신하면, 상기 타이머가 타이밍을 중단하고 리셋하는 것을 특징으로 하는 네트워크 주소 변환 게이트웨이.

청구항 3. 제 1 항에 있어서,

상기 외부 네트워크는 인터넷인 것을 특징으로 하는 네트워크 주소 변환 게이트웨이.

청구항 4. 제 3 항에 있어서,

상기 랜은 가상 사설 네트워크인 것을 특징으로 하는 네트워크 주소 변환 게이트웨이.

청구항 5. 로컬 IP 주소를 사용하는 랜 상의 로컬 장치로부터 네트워크 변환 게이트웨이를 거쳐 외부 네트워크 상의 외부 장치로 IP 데이터그램을 처리하는 방법에 있어서,

상기 랜 상의 로컬 장치들의 로컬 IP 주소들, 상기 외부 네트워크 상의 외부 장치들의 외부 IP 주소들, 상기 로컬 장치들의 포트 주소들, 상기 외부 장치들의 포트 주소들, SPI-In 값들, SPI-Out 값들 및 예약된 포트 주소들 및 예약된 포트 주소들의 리스트를 결합하는 복수개의 테이블들을 유지하는 단계;

상기 랜으로부터 데이터그램을 수신하는 단계;

상기 데이터그램이 암호화되어 있는 지를 결정하고, 상기 데이터그램이 암호화되어 있으면, 상기 데이터그램의 SPI가 상기 복수개의 내부 테이블들 중의 하나의 SPI-Out 필드에 기록되어 있는 지를 결정하고, 상기 데이터그램의 SPI가 상기 내부 테이블의 상기 SPI-Out 필드에 기록되어 있으면, 상기 소스 IP 주소를 상기 게이트웨이의 외부 IP 주소가 되도록 변경하고, 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하고,

상기 SPI가 상기 내부 테이블의 상기 SPI-Out 필드에 기록되어 있지 않으면 상기 외부 장치의 IP 주소에 해당하는 SPI-Out 필드를 상기 SPI와 동일하게 세팅하고 상기 내부 테이블의 SPI-In 필드를 0으로 세팅하고, 상기 소스 IP 주소를 상기 게이트웨이의 상기 외부 IP 주소가 되도록 변경하고, 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하고,

상기 데이터그램이 암호화되어 있지 않으면, 상기 데이터그램을 위한 목적지 포트 주소가 예약된 포트 주소들의 상기 테이블에 포함되어 있는 지를 결정하고, 상기 목적지 포트 주소가 예약된 포트 주소들의 상기 테이블에 포함되어 있지 않으면, 상기 데이터그램에 대해 일반 주소 변환을 수행하고 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하고,

상기 목적지 포트 주소가 예약된 포트 주소들의 상기 테이블에 포함되어 있으면, 상기 목적지 포트 주소가 IP 주소에 구속되어 있는 지를 결정하고, 상기 목적지 포트 주소가 IP 주소에 구속되어 있으면, 상기 데이터그램에 대해 일반 주소 변환을 수행하고, 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하고,

상기 목적지 포트 주소가 IP 주소에 구속되어 있지 않으면, 상기 소스 IP 주소를 상기 외부 장치를 위한 상기 외부 IP 주소가 되도록 변경하고, 상기 목적지 포트 주소를 상기 로컬 장치의 상기 로컬 IP 주소에 구속하고 상기 목적지 포트 주소와 상기 외부 장치의 상기 외부 IP 주소 사이의 연결을 만들고, 상기 외부 장치로 라우팅하고 전달하기 위한 상기 외부 네트워크로 상기 데이터그램을 전송하는 단계를 포함하는 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 6. 외부 네트워크 상의 외부 장치로부터 네트워크 변환 게이트웨이를 거쳐 로컬 IP 주소들을 사용하는 랜 상의 로컬 장치로 IP 데이터그램을 처리하는 방법에 있어서,

상기 랜 상의 로컬 장치들의 로컬 IP 주소들, 상기 외부 네트워크 상의 외부 장치들의 외부 IP 주소들, 상기 로컬 장치들의 포트 주소들, 상기 외부 장치들의 포트 주소들, SPI-In 값들, SPI-Out 값들 및 예약

된 포트 주소들 및 예약된 포트 주소들의 리스트를 결합하는 복수개의 테이블들을 유지하는 단계;

상기 네트워크로부터 데이터그램을 수신하는 단계;

상기 데이터그램이 암호화되어 있는 지를 결정하고, 상기 데이터그램이 암호화되어 있으면, 상기 데이터그램의 SPI가 상기 복수개의 내부 테이블들 중의 하나의 SPI-In 필드에 기록되어 있는 지를 결정하고, 상기 데이터그램의 SPI가 상기 내부 테이블의 상기 SPI-In 필드에 기록되어 있으면, 상기 목적지 IP 주소를 상기 로컬 장치의 내부 IP 주소가 되도록 변경하고, 상기 로컬 장치로 라우팅하고 전달하기 위한 상기 랜으로 상기 데이터그램을 전송하고,

상기 SPI가 상기 내부 테이블의 상기 SPI-In 필드에 기록되어 있지 않으면 상기 외부 장치의 IP 주소에 해당하는 SPI-In 필드가 0인지를 결정하고 상기 SPI-In 필드가 0이 아니면, 상기 데이터그램을 버리고,

상기 SPI-In 필드가 0이면, 상기 SPI-In 필드를 상기 SPI가 되도록 변경하고, 상기 목적지 IP 주소를 상기 로컬 장치의 상기 로컬 IP 주소가 되도록 변경하고, 상기 로컬 장치로 라우팅하고 전달하기 위한 상기 랜으로 상기 데이터그램을 전송하고,

상기 데이터그램이 암호화되어 있지 않으면, 상기 데이터그램을 위한 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있는 지를 결정하고, 상기 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있지 않으면, 일반 주소 변환을 수행하고 상기 로컬 장치로 라우팅하고 전달하기 위한 상기 랜으로 상기 데이터그램을 전송하고,

상기 목적지 포트 주소가 예약된 포트 주소들의 상기 리스트에 포함되어 있으면, 상기 목적지 포트 주소가 상기 로컬 IP 주소에 구속되어 있는 지를 결정하고, 상기 목적지 포트 주소가 상기 로컬 IP 주소에 구속되어 있지 않으면, 상기 데이터그램을 버리고,

상기 목적지 포트 주소가 IP 주소에 구속되어 있으면, 상기 IP 주소를 상기 로컬 장치의 상기 로컬 IP 주소가 되도록 변경하고, 상기 로컬 IP 주소로부터의 상기 목적지 포트 주소에 대한 구속을 해제하고, 상기 로컬 장치로 라우팅하고 전달하기 위한 상기 랜으로 상기 데이터그램을 전송하는 단계를 포함하는 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 7. 제 5 항에 있어서,

상기 목적지 포트 주소가 상기 로컬 장치의 상기 로컬 IP 주소에 구속될 때마다 타이머를 시작하는 단계;

상기 목적지 포트 주소가 해제될 때마다 상기 타이머를 리셋팅하는 단계; 및

상기 타이머가 동작중이고 미리 지정된 시간이 상기 타이머가 시작한 시점으로부터 종료될 때마다 신호를 전송하는 단계를 더 포함하는 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 8. 제 6 항에 있어서,

상기 목적지 포트 주소가 상기 로컬 장치의 상기 로컬 IP 주소에 구속될 때마다 타이머를 스타트시키는 단계;

상기 목적지 포트 주소가 릴리스될 때마다 상기 타이머를 리셋팅하는 단계; 및

상기 타이머가 동작중이고 미리 지정된 시간이 상기 타이머가 스타트한 시점으로부터 종료될 때마다 신호를 전송하는 단계를 더 포함하는 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 9. 제 5 항에 있어서,

상기 외부 네트워크가 인터넷인 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 10. 제 6 항에 있어서,

상기 외부 네트워크가 인터넷인 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 11. 제 5 항에 있어서,

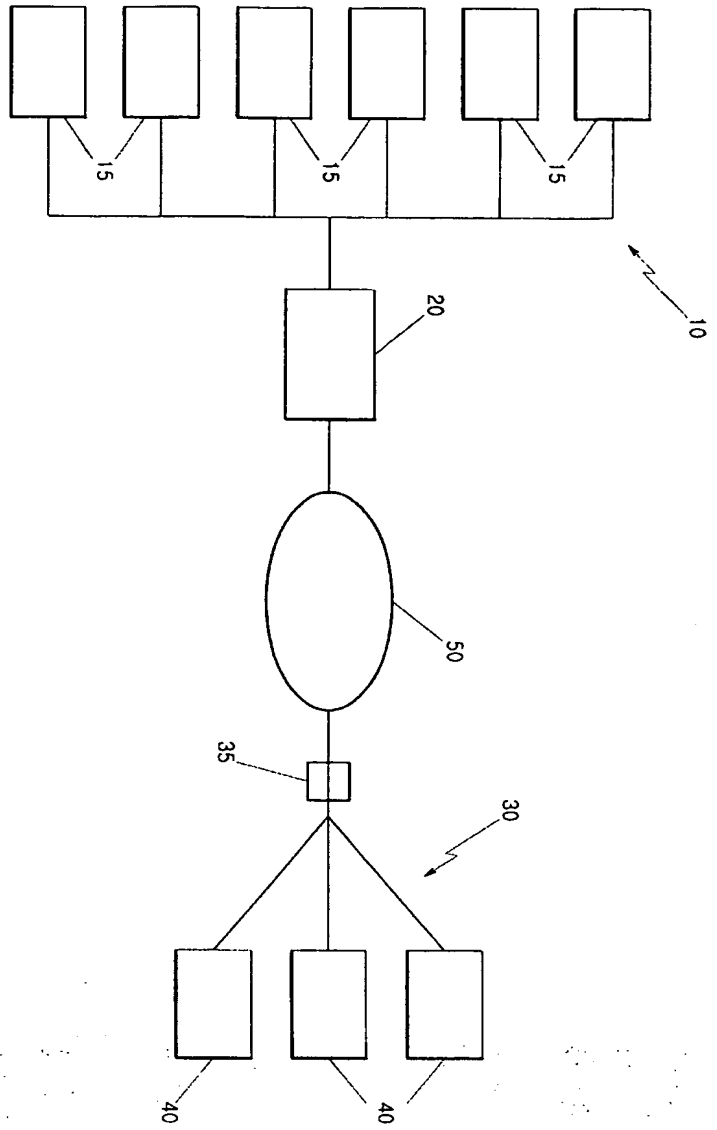
상기 랜이 가상 사설 네트워크인 것을 특징으로 하는 IP 데이터그램 처리 방법.

청구항 12. 제 6 항에 있어서,

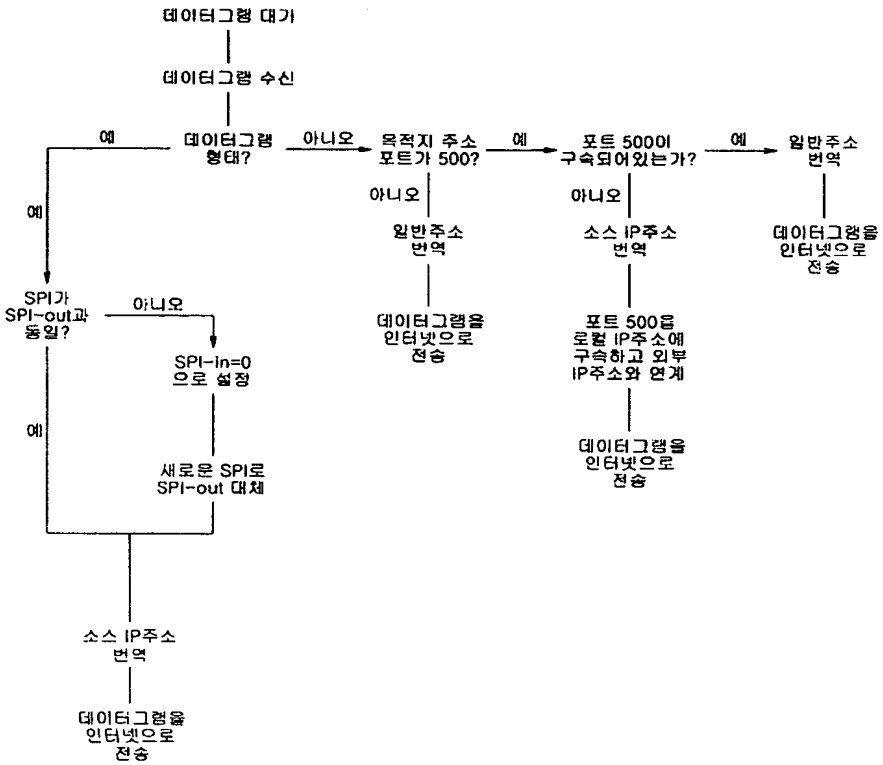
상기 랜이 가상 사설 네트워크인 것을 특징으로 하는 IP 데이터그램 처리 방법.

도면

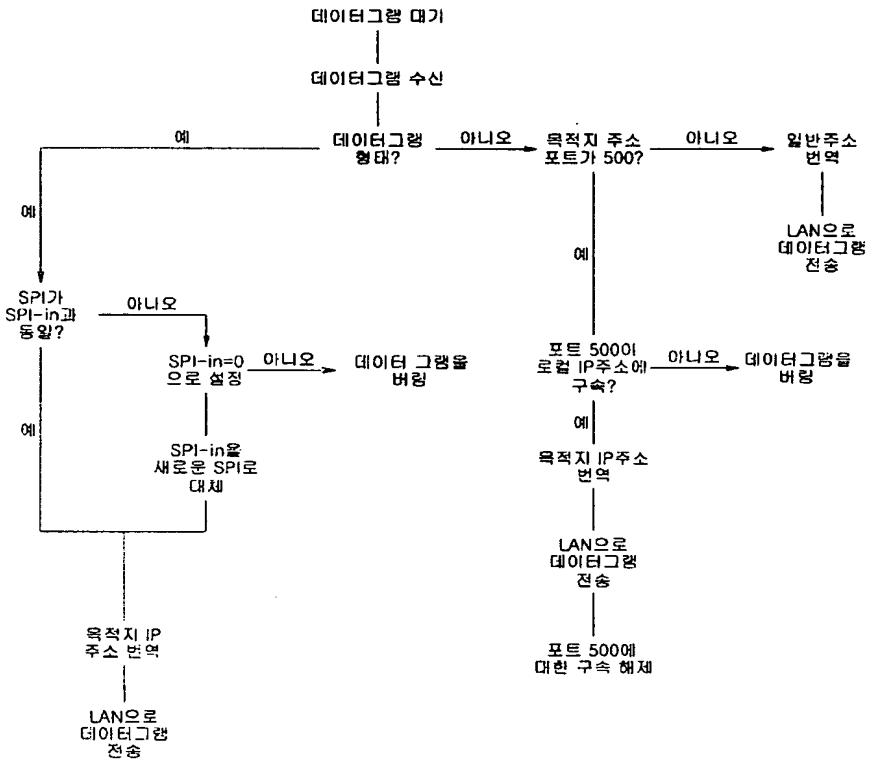
도면1



도면2


데이터그램 대기
데이터그램 수신
데이터그램 형태?
예
아니오
목적지 주소 포트가 500?
예
포트 500이 구속되어있는가?
예
일반주소 번역
아니오
일반주소 번역
데이터그램을 인터넷으로 전송
아니오
소스 IP주소 번역
포트 500을 로컬 IP주소에 구속하고 외부 IP주소와 연계
데이터그램을 인터넷으로 전송
데이터그램을 인터넷으로 전송
예
SPI가 SPI-out과 동일?
아니오
SPI-in=0 으로 설정
예
새로운 SPI로 SPI-out 대체
소스 IP주소 번역
데이터그램을 인터넷으로 전송

도면3



도면4

IP주소

	로컬 컴퓨터	게이트웨이 내부	게이트웨이 외부	타겟	
L-1	192.168.0.2	102.168.0.1	142.140.3.6	204.71.202.160	T-1
L-2	192.168.0.4	102.168.0.1	142.140.3.6	207.46.131.137	T-2
L-3	192.168.0.3	102.168.0.1	142.140.3.6	207.158.227.235	T-3

도면5a

테이블 3개의 호스트와 통신하는 8개의 로컬 컴퓨터

	타겟	로컬 IP		SPI-out	SPI-in
T-1	204.71.202.160	192.168.0.2	L-1	4859	9802
		102.168.0.5	L-x	52856	7000
		102.168.0.10	L-x	8565	8523
T-2	207.46.131.137	192.168.0.4	L-2	1353	6234
		102.168.0.7	L-x	2562	10125
		102.168.0.10	L-x	25763	12106
T-3	207.158.227.235	192.168.0.3	L-3	38935	7753
		102.168.0.8	L-x	9093	32828

도면5b

새로운 세션 - 새로운 SPI-out - SPI-in을 0으로 설정

	타겟	로컬 IP		SPI-out	SPI-in
T-1	204.71.202.160	192.168.0.2	L-1	14662	0
		102.168.0.5	L-x	52856	7000
		102.168.0.10	L-x	8565	8523
T-2	207.46.131.137	192.168.0.4	L-2	1353	4562
		102.168.0.7	L-x	2562	10125
		102.168.0.10	L-x	25763	12106
T-3	207.158.227.235	192.168.0.3	L-3	8773	20889
		102.168.0.8	L-x	9093	32828

도면5c

수신된 응답 패킷-수신된 새로운 SPI-in

	타겟	로컬 IP		SPI-out	SPI-in
T-1	207.200.0.2	192.168.0.2	L-1	14662	3288
		102.168.0.5	L-x	52856	7000
		102.168.0.10	L-x	8565	8523
T-2	206.23.5.120	192.168.0.4	L-2	1353	6234
		102.168.0.7	L-x	43966	17937
		102.168.0.10	L-x	25763	12106
T-3	207.198.75.3	192.168.0.3	L-3	8773	20889
		102.168.0.8	L-x	9093	32828

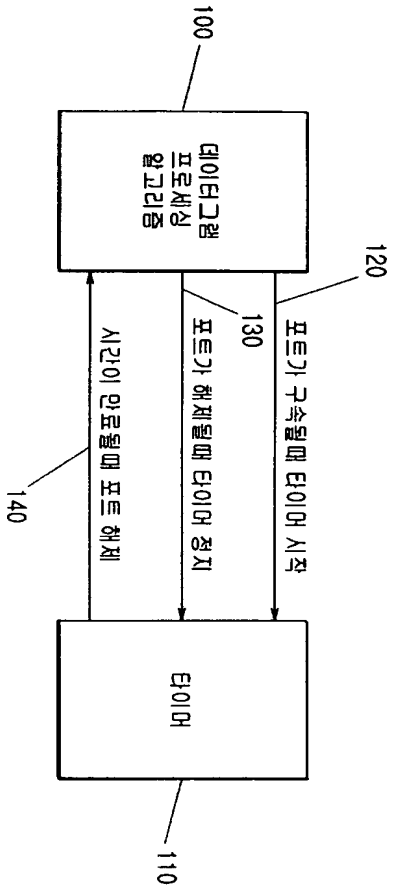
도면6

게이트웨이를 통한 패킷의 순서 하나의 로컬 장비 - 하나의 목표							
경로	데이터그램 형태	소스 주소 IP	포트	목적지 주소 IP	포트	SPI	줄
LAN-Gate	UDP	192.168.0.2	6404	204.71.202.160	80		1
Gate-Net	UDP	142.140.3.6	10425	204.71.202.160	80		2
LAN-Gate	UDP	204.71.202.160	80	142.140.3.6	10425		3
Gate-LAN	UDP	204.71.202.160	80	192.168.0.2	6404		4
LAN-Gate	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		5
Gate-Net	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		6
Net-Gate	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		7
Gate-LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		8
LAN-Gate	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		9
Gate-Net	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		10
Net-Gate	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		11
Gate-LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		12
LAN-Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		13
Gate-Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		14
Net-Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		15
Gate-LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		16
LAN-Gate	ESP(50)	192.168.0.2		204.71.202.160		4859	17
Gate-Net	ESP(50)	142.140.3.6		204.71.202.160		4859	18
Net-Gate	ESP(50)	204.71.202.160		142.140.3.6		9802	19
Gate-LAN	ESP(50)	204.71.202.160		192.168.0.2		9802	20
LAN-Gate	ESP(50)	192.168.0.2		204.71.202.160		4859	21
Gate-Net	ESP(50)	142.140.3.6		204.71.202.160		4859	22
Net-Gate	ESP(50)	204.71.202.160		142.140.3.6		9802	23
Gate-LAN	ESP(50)	204.71.202.160		192.168.0.2		9802	24
LAN-Gate	ESP(50)	192.168.0.2		204.71.202.160		14662	25
Gate-Net	ESP(50)	142.140.3.6		204.71.202.160		14662	26
Net-Gate	ESP(50)	204.71.202.160		142.140.3.6		3288	27
Gate-LAN	ESP(50)	204.71.202.160		192.168.0.2		3288	28
LAN-Gate	ESP(50)	192.168.0.2		204.71.202.160		14662	29
Gate-Net	ESP(50)	142.140.3.6		204.71.202.160		14662	30
Net-Gate	ESP(50)	204.71.202.160		142.140.3.6		3288	31
Gate-LAN	ESP(50)	204.71.202.160		192.168.0.2		3288	32

도면7

게이트웨이를 통한 패킷의 순서 복수의 로컬 장비 - 복수의 목표								
경로	패킷 형태	소스 주소 IP	서비스	목적지 주소 IP	서비스	SPI	실행중인 프로세스	줄
LAN-Gate	UDP	192.168.0.2	6404	204.71.202.160	80		L-1 Out	1
Gate-Net	UDP	142.140.3.6	10425	204.71.202.160	80		T-1 In	2
LAN-Gate	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 Out	3
Gate-Net	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 In	4
Net-Gate	UDP	204.71.202.160	80	142.140.3.6	10425		T-1 Out	5
Gate-LAN	UDP	204.71.202.160	80	192.168.0.2	6404		L-1 In	6
Net-Gate	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 Out	7
Gate-LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 In	8
LAN-Gate	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		L-1 Out- 포트5000이 192.168.0에 구속	9
Gate-Net	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		T-1 In- 204.71.202.160에 결합	10
Net-Gate	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		T-1 Out	11
Gate-LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		L-1 In- 포트 500 해제	12
LAN-Gate	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		L-1 Out- 포트5000이 192.168.0에 구속	13
Gate-Net	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		T-1 In- 204.71.202.160에 결합	14
LAN-Gate	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 Out	15
Gate-Net	ISAKMP-1	142.140.3.6	500	207.158.227.235	8773		T-3 In- 포트 500 사용불가	16
Net-Gate	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		T-1 Out	17
Gate-LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		L-1 In- 포트 500 해제	18
LAN-Gate	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 Out	19
Gate-Net	ISAKMP-1	142.140.3.6	500	207.158.227.235	500		T-3 In- 포트5000이 192.168.0.3에 구속	20
LAN-Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out- 포트 500 사용불가	21
Gate-Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	9063		T-1 In- 소스 포트 주소 변역	22
Net-Gate	ISAKMP-2	207.158.227.235	500	142.140.3.6	500		T-3 Out	23
Gate-LAN	ISAKMP-2	207.158.227.235	500	192.168.0.2	500		L-1 In- 포트 500 해제	24
LAN-Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out- 포트5000이 192.168.0에 구속	25
Gate-Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 In- 204.71.202.160에 결합	26
							T-1 타임아웃, 포트 500 해제	27
LAN-Gate	ISAKMP-3	192.168.0.3	500	207.158.227.235	500		L-3 Out	28
Gate-Net	ISAKMP-3	142.140.3.6	500	207.158.227.235	500		T-3 In- 포트5000이 192.168.0.3에 구속	29
Net-Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 Out- 포트5000에 막힘	30
							T-1 Out- 패킷 무시	31
Net-Gate	ISAKMP-4	207.158.227.235	500	142.140.3.6	500		T-3 Out	32
Gate-LAN	ISAKMP-4	207.158.227.235	500	192.168.0.3	500		L-3 In- 포트 500 해제	33
LAN-Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out- 포트5000이 192.168.0에 구속	34
Gate-Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 In- 204.71.202.160에 결합	35
Net-Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 Out	36
Gate-LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		L-1 In- 포트 500 해제	37
LAN-Gate	ESP(50)	192.168.0.2		204.71.202.160		4859	L-1 Out	38
Gate-Net	ESP(50)	142.140.3.6		204.71.202.160		4859	T-1 In	39
LAN-Gate	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 Out	40
Gate-Net	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 In	41
Net-Gate	ESP(50)	204.71.202.160		142.140.3.6		9802	T-1 Out	42
Gate-LAN	ESP(50)	204.71.202.160		192.168.0.2		9802	L-1 In	43
LAN-Gate	ISAKMP-5	192.168.0.3	500	207.158.227.235	500		L-3 Out- 포트5000이 192.168.0.3에 구속	44
Gate-Net	ISAKMP-5	142.140.6.3	500	207.158.227.235	500		T-3 In- 207.158.227.23에 결합	45
LAN-Gate	ESP(50)	192.168.0.2		204.71.202.160		4859	L-1 Out	46
Gate-Net	ESP(50)	142.140.3.6		204.71.202.160		4859	T-1 In	47
Net-Gate	ISAKMP-6	207.158.227.235	500	142.140.3.6	500		T-3 Out	48
Gate-LAN	ISAKMP-6	207.158.227.235	500	192.168.0.3	500		L-3 In- 포트 500 해제	49
LAN-Gate	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 Out	50
Gate-Net	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 In	51
LAN-Gate	ESP(50)	192.168.0.3		207.158.227.235		38935	L-3 Out	52
Gate-Net	ESP(50)	142.140.6.3		207.158.227.235		38935	T-3 In	53
Net-Gate	ESP(50)	204.71.202.160		142.140.3.6		9802	T-1 Out	54
Gate-LAN	ESP(50)	204.71.202.160		192.168.0.2		9802	L-1 In	55
Net-Gate	ESP(50)	207.158.227.235		142.140.3.6		7753	T-3 Out	56
Gate-Net	ESP(50)	207.158.227.235		192.168.0.3		7753	L-3 In	57

도면8


100
데이터그램 프로세싱 알고리즘
120
130
포트가 구속될때 타이머 시작
포트가 해제될때 타이머 정지
시간이 만료될때 포트 해제
140
타이머
110